

**THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Appellant: Martina Hanck et al.
Appl. No.: 09/402,144
Conf. No.: 5593
Filed: September 29, 1999
Title: METHOD AND SYSTEM FOR PRODUCING AND CHECKING A HASH
TOTAL FOR DIGITAL DATA GROUPED IN SEVERAL DATA SEGMENTS
Art Unit: 2132
Examiner: J.W. Kim
Docket No.: 112740-466

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' APPEAL BRIEF

Sir:

Appellants submit this Appeal Brief in support of the Notice of Appeal filed on September 27, 2007, along with the Pre-Appeal Brief Request for Review. This Appeal is taken from the Final Rejection in the Office Action dated June 27, 2007 and Notice of Panel Decision from Pre-Appeal Brief Review dated November 28, 2007.

I. REAL PARTY IN INTEREST

The real party in interest for the above-identified patent application on Appeal is Siemens Aktiengesellschaft (“Siemens AG”) by virtue of an Assignment dated February 3, 1998 and recorded at reel 010411, frame 0669 in the United States Patent and Trademark Office.

II. RELATED APPEALS AND INTERFERENCES

Appellants' legal representative and the Assignee of the above-identified patent application do not know of any prior or pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision with respect to the above-identified Appeal.

III. STATUS OF CLAIMS

Claims 1-3, 10-12, 22-33 and 37-48 are pending in the above-identified patent application. Claims 4-9, 13-21 and 34-36 have been canceled. Claims 1-3, 10-12, 22-33 and 37-48 have been rejected. Accordingly, Claims 1-3, 10-12, 22-33 and 37-48 are being appealed in this Brief. A copy of the appealed claims is included in the Claims Appendix.

IV. STATUS OF AMENDMENTS

No amendments were made to the claims on appeal subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A summary of the invention by way of reference to the drawings and specification for each of the independent claims and each means plus function claim may be found in Appendix B to this Brief.

Although specification citations are given in accordance with C.F.R. 1.192(c), these reference numerals and citations are merely examples of where support may be found in the specification for the terms used in this section of the Brief. There is no intention to suggest in any way that the terms of the claims are limited to the examples in the specification. As demonstrated by the references numerals and citations below, the claims are fully supported by the specification as required by law. However, it is improper under the law to read limitations from the specification into the claims. Pointing out specification support for the claim terminology as is done here to comply with rule 1.192(c) does not in any way limit the scope of the claims to those examples from which they find support. Nor does this exercise provide a mechanism for circumventing the law precluding reading limitations into the claims from the specification. In short, the references numerals and specification citations are not to be construed as claim limitations or in any way used to limit the scope of the claims.

Claim 1

With reference to the figure, claim 1 recites a method for securely controlling transmission of digital data (pg. 9, lines 7-12). The method includes the steps of receiving said digital data (pg. 7, lines 4-9), grouping said digital data into a number of data segments by a computer (pg. 7, lines 14-16), forming a first segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, 16-20 and pg 10, lines 1-7), forming a first commutative checksum by a commutative operation on said first segment checksums (pg, 7, lines 20-25), wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and cryptographically protecting said first commutative checksum by using a cryptographic operation (pg. 7, lines 24-30).

Claim 2

With reference to the figure, claim 2 recites a method for securely controlling transmission of digital data (pg. 9, lines 7-12). The method includes the steps of receiving said digital data (pg. 7, lines 4-9), grouping the digital data into a number of data segments by a computer (pg. 7, lines 14-16), allocating a predetermined cryptographic commutative checksum to said digital data (pg 7, lines, 16-20), subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum (pg. 7, lines 24-30 and pg 8, lines 13-18), forming a second segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 8, lines 7-12 and pg 10, lines 1-8), forming a second commutative checksum by a commutative operation on said second segment checksums (pg 9, lines 1-3), wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and checking said second commutative checksum for a match with said first commutative checksum. (pg. 9, lines 4-6).

Claim 3

With reference to the figure, claim 3 recites a method for forming and checking a first commutative checksum for digital data (pg. 9, lines 4-6). The method includes the steps of grouping said digital data into a number of data segments by a computer (pg. 7, lines 14-16), forming a first segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, 16-20 and pg 10, lines 1-7), forming said first commutative checksum by a commutative operation on said first segment checksums (pg. 7, lines 20-25), wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), cryptographically protecting said first commutative checksum by using at least one cryptographic operation, which forms a cryptographic commutative checksum (pg. 7, lines 24-30), subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a reconstructed first commutative checksum (pg 8, lines 13-18), forming a second segment checksum for each said data segment of said digital data to which said first commutative checksum is allocated (pg 8, lines 7-12 and pg 10, lines 1-8), forming a second commutative checksum by a commutative operation on said second segment checksums (pg. 9, lines 1-3), wherein flow control for the data

segments is negated by the commutative operation (pg. 2, lines 14-26), and checking said second commutative checksum for a match with said reconstructed first commutative checksum (pg. 9, lines 4-6).

Claim 10

With reference to the figure, claim 10 recites an arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments (pg 7, lines 16-25). The arrangement includes an arithmetic and logic unit (R; pg 7, lines 10-15), a first segment checksum (PS1-PSn; pg. 7, lines 16-20), which is formed for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, 16-20 and pg 10, lines 1-7), a commutative operation which forms said first commutative checksum by operating on said segment checksums (101; pg 7, lines 31-35) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and a cryptographic operation which cryptographically protects said first commutative checksum (pg. 7, lines 24-30).

Claim 11

With reference to the figure, claim 11 recites an arrangement for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments (pg 9, lines 4-6). The arrangement includes an arithmetic and logic unit (R; pg 7, lines 10-15), a first segment checksum (PS1-PSn; pg. 7, lines 16-20), formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, 16-20 and pg 10, lines 1-7), an inverse cryptographic operation to form a first cryptographic checksum from a cryptographic commutative checksum formed by a cryptographic operation (pg. 7, lines 24-30) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), a second segment checksum which is formed for each said data segment wherein said second segment checksum is formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (PSa-Psz; pg 8, lines 7-12 and pg 10, lines 1-8), a commutative operation which operates on said second segment checksums which forms a second commutative checksum (pg 9, lines 1-3) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and a comparator which checks for a

match between said second commutative checksum and said first commutative checksum (pg 9, lines 4-6).

Claim 12.

With reference to the figure, claim 12 recites an arrangement for forming and checking a first commutative checksum for digital data which is grouped into a number of data segments (pg. 9, lines 4-6). The arrangement includes an arithmetic and logic unit (R; pg 7, lines 10-15), a first segment checksum (PS1-PSn; pg. 7, lines 16-20), which is formed for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg 7, lines, 16-20 and pg 10, lines 1-7), a commutative operation which forms said first commutative checksum by operating on said first segment checksums (101; pg 7, lines 31-35) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), a cryptographic operation which cryptographically protects said first commutative checksum (pg. 7, lines 24-30), a cryptographic commutative checksum formed by said cryptographic operation (KP; pg 7, lines 26-30); an inverse cryptographic operation to form a first commutative checksum from said cryptographic commutative checksum (pg. 7, lines 24-30), a second segment checksum which is formed for each said data segment of said digital data to which said first commutative checksum is allocated (pg 8, lines 7-12 and pg. 10, lines 1-8), a commutative operation which operates on said second segment checksums which forms a second commutative checksum (pg. 9, lines 1-3) wherein flow control for the data segments is negated by the commutative operation (pg. 2, lines 14-26), and a comparator which checks for a match between said second commutative checksum and a reconstructed first commutative checksum (pg 9, lines 4-6), wherein said first and second segment checksum are formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function (pg. 10, lines 1-8).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-3, 10-12, 22-33 and 37-48 stand rejected under 35 USC §103(a) as being unpatentable over USPN 5,649,089 to Kilner in view of USPN 4,982,430 to Frezza; the subject matter of USPN to McNamara et al. is relied upon since McNamara is incorporated by reference in Frezza.

VII. ARGUMENT

LEGAL STANDARDS

1. Obviousness under 35 U.S.C. §103

The Federal Circuit has held that the legal determination of an obviousness rejection under 35 U.S.C. § 103 is:

whether the claimed invention as a whole would have been obvious to a person of ordinary skill in the art at the time the invention was made...The foundational facts for the *prima facie* case of obviousness are: (1) the scope and content of the prior art; (2) the difference between the prior art and the claimed invention; and (3) the level of ordinary skill in the art...Moreover, objective indicia such as commercial success and long felt need are relevant to the determination of obviousness...Thus, each obviousness determination rests on its own facts.

In re Mayne, 41 U.S.P.Q. 2d 1451, 1453 (Fed. Cir. 1997).

In making this determination, the Patent Office has the initial burden of proving a *prima facie* case of obviousness. *In re Rijckaert*, 9 F.3d 1531, 1532, 28 U.S.P.Q. 2d 1955, 1956 (Fed. Cir. 1993). This burden may only be overcome “by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings.” *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir. 1988). “If the examination at the initial stage does not produce a *prima facie* case of unpatentability, then without more the Appellant is entitled to grant of the patent.” *In re Oetiker*, 24 U.S.P.Q. 2d 1443, 1444 (Fed. Cir. 1992).

Moreover, the Patent Office must provide explicit reasons why the claimed invention is obvious in view of the prior art. The Supreme Court has emphasized that when formulating a rejection under 35 U.S.C. § 103(a) based upon a combination of prior art elements it remains necessary to identify the reason why a person of ordinary skill in the art would have combined the prior art elements in the manner claimed. *KSR v. Teleflex*, 127 S. Ct. 1727 (2007).

Of course, references must be considered as a whole and those portions teaching against or away from the claimed invention must be considered. *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve Inc.*, 796 F.2d 443 (Fed. Cir. 1986). “A prior art reference may be considered to teach away when a person of ordinary skill, upon reading the reference would be discouraged

from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the Appellant.” *Monarch Knitting Machinery Corp. v. Fukuhara Industrial Trading Co., Ltd.*, 139 F.3d 1009 (Fed. Cir. 1998), quoting, *In re Gurley*, 27 F.3d 551 (Fed. Cir. 1994).

B. THE REJECTION OF CLAIMS 1-3, 10-12, 22-33 and 37-48 UNDER 35 U.S.C. §103(A) SHOULD BE REVERSED, BECAUSE KILNER, FREZZA AND MCNAMARA FAIL TO RENDER THE CLAIMS OBVIOUS

None of the cited art, alone or in combination teaches or suggests the feature of performing a commutative operation on segment checksums, wherein flow control for the data segments is negated by the commutative operation. Under the claimed configuration, by using the commutative operation for individual checksums of the data segments, flow control for the order of the individual data segments is no longer required.

In contrast, *Kilner* proposes a cumulative checksum process that relies on flow control of individual data segments (col. 1, lines 41-55; col. 2, lines 44-55; col. 3, lines 51-65), as each checksum is specifically directed to changes in specific places of a record database and affiliating an old checksum value from the cumulative checksum (see claim 1). *Kilner* discloses the real time tracking of changes to redundant databases, where a data communication system has an active controller 112 and a standby controller 115 (FIG. 1). The standby controller 115 assumes the role of the active controller in the event that the active controller experiences a failure within the system. *Kilner* discloses that, in the case where the active controller becomes disabled, the standby controller must be capable of performing the functions of the active controller, and “in order to effectively and efficiently perform the function of the active controller, the standby controller must be a substantially exact duplicate of the active controller, thus a redundant or standby database controller system must exist” (col. 2, lines 19-25). Thus, to track modifications in the databases, *Kilner* relies on virtual checksums to affirm an active checksum with a standby checksum in a record database (col. 2, lines 35-55).

While the Final Office Action argues that checksums A_CRC, V_CRC and S_CRC are not dependent on the ordering of the data, Appellant maintains that the redundant databases requires the system in *Kilner* to perform cumulative checksums on the database (DB) with the

(identical or “mirror image”) standby DB to track changes and to set-up the reversible record checksum (col. 3, lines 52-65; see col. 4, lines 66-67). The present claims recite performing a commutative operation on segment checksums, which is not taught or suggested in Kilner. Each of the checksums (A_CRC, V_CRC and S_CRC) are disclosed as being cumulative checksums (col. 3, lines 52-65; see claim 1: all checksums are “cumulative”). While the Final Office Action argues that Kilner discloses a commutative checksum (i.e., that the “cumulative checksum” appears in name only - see page 3, paragraph 4), Appellant respectfully submits this is incorrect.

The Office Action cites col. 3, lines 52-55 and the XOR operation as the equivalent of the claimed commutative checksum. However, Appellant points out that the XOR operation is only applied to the reversible incorporation of record checksums (R_CRC), where the checksums are “backed in” and “backed out” of the A_CRC checksum, which is disclosed as the “cumulative checksum of the entire DB for substantially real time tracking changes to a database” (col. 3, lines 53-55). The R_CRC checksum then, must rely on flow control, since the individual records must be ordered to update the record numbers in the A_CRC (col. 4, lines 27-54).

Furthermore, the CRC’s of Kilner are not disclosed as having any cryptographic characteristics. The entire disclosure of Kilner is concerned with preventing “lock out” and maintaining the integrity of a database associated with a standby controller when multiple changes are effected on the database record and corresponding backup (col. 1, lines 17-27, 41-54). Nothing in the disclosure of Kilner addresses cryptographic security. In the previous response, it was argued that Kilner “secures” the database by performing the CRC check with an XOR function on two identical databases (col. 4, .lines 66-67). Thus, an alteration to one of the databases would trigger a reset/resync in the system (col. 5, lines 3-7). The Office Action fails to explain how the record checksum (R_CRC, ref. 124) has any hashing or cryptographic characteristics.

Frezza and McNamara fail to solve the deficiencies of Kilner as well. *Frezza* deals with a configuration for securely downloading data from a remote site, where booter data for a CATV system is downloaded to a terminal to establish subscriber identity (col. 4, lines 18-36) The checksum is merely performed to merely validate the user to establish a communication link (col. 5, line 39 - col. 6, line 19). The disclosure in McNamara merely discloses a conventional DES encryption/decryption scheme which secures a connection over a data channel on a CATV system (col. 7, lines 26-42; col. 8, lines 36-48). The Office Action does not explain how Frezza

or McNamara could possibly be incorporated into the redundant database system of Kilner. The redundancy checksum of Kilner (R_CRC) merely bridges the “old” record with the “new” record checksum in a cumulative manner (but not commutatively) to resolve updated data records (col. 4, lines (col. 4, lines 27-54).

Appellant submits that there is no apparent reason to combine the references in the manner suggested in the Office Action. “[A] patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.” KSR Int’l Co. v. Teleflex Inc. 550 U.S. ____ (2007). The Office Action fails to provide a valid reason why a person of ordinary skill in the art would have combined the prior art elements in the manner claimed. The Office Action states that it would have been obvious to make the combination “to prevent an unauthorized modification of a transmitted message” (page 5, lines 5-7; page 6, paragraph 13, *et al.*). However, as explained above, Kilner does not appear to have anything to do with the external transmission of messages, but only appears to disclose a system for internally resolving updates to redundant databases. Kilner is not concerned with who is modifying the messages - the disclosure in Kilner only addresses whether or not the databases are consistent with their content (col. 2, lines 44-56).

VIII. CONCLUSION

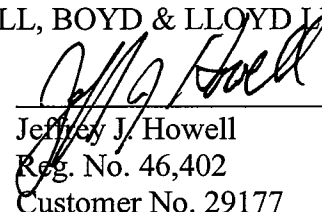
Appellants respectfully submit that Claims 1-3, 10-12, 22-33 and 37-48 are non-obvious in view of the cited references for the reasons previously discussed. Accordingly, Appellants respectfully submit that the rejections under 35 U.S.C. §103(a) are erroneous in law and in fact and should therefore be reversed by this Board.

The Director is authorized to charge any additional fees which may be required, or to credit any overpayment to Deposit Account No. 02-1818. If such a withdrawal is made, please indicate the Attorney Docket No. 112740-466 on the account statement.

Respectfully submitted,

BELL, BOYD & LLOYD LLP

BY


Jeffrey J. Howell

Reg. No. 46,402

Customer No. 29177

Dated: January 28, 2008

CLAIMS APPENDIX

Claim 1. A method for securely controlling transmission of digital data comprising the steps of:

- receiving said digital data;
- grouping said digital data into a number of data segments by a computer;
- forming a first segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;
- forming a first commutative checksum by a commutative operation on said first segment checksums, wherein flow control for the data segments is negated by the commutative operation;
- and
- cryptographically protecting said first commutative checksum by using a cryptographic operation.

Claim 2. A method for securely controlling transmission of digital data comprising the steps of:

- receiving said digital data;
- grouping the digital data into a number of data segments by a computer;
- allocating a predetermined cryptographic commutative checksum to said digital data;
- subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum;
- forming a second segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;
- forming a second commutative checksum by a commutative operation on said second segment checksums wherein flow control for the data segments is negated by the commutative operation; and
- checking said second commutative checksum for a match with said first commutative checksum.

Claim 3. A method for forming and checking a first commutative checksum for digital data comprising the steps of:

grouping said digital data into a number of data segments by a computer;

forming a first segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;

forming said first commutative checksum by a commutative operation on said first segment checksums, wherein flow control for the data segments is negated by the commutative operation;

cryptographically protecting said first commutative checksum by using at least one cryptographic operation, which forms a cryptographic commutative checksum;

subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a reconstructed first commutative checksum;

forming a second segment checksum for each said data segment of said digital data to which said first commutative checksum is allocated;

forming a second commutative checksum by a commutative operation on said second segment checksums wherein flow control for the data segments is negated by the commutative operation; and

checking said second commutative checksum for a match with said reconstructed first commutative checksum.

Claims 4-9 (canceled).

Claim 10. An arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments, said arrangement comprising:

an arithmetic and logic unit,

a first segment checksum, which is formed for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function,

a commutative operation which forms said first commutative checksum by operating on said segment checksums wherein flow control for the data segments is negated by the commutative operation, and

a cryptographic operation which cryptographically protects said first commutative checksum.

Claim 11. An arrangement for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments, said arrangement comprising:

- an arithmetic and logic unit;
- a first segment checksum, formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;
- an inverse cryptographic operation to form a first cryptographic checksum from a cryptographic commutative checksum formed by a cryptographic operation wherein flow control for the data segments is negated by the commutative operation;
- a second segment checksum which is formed for each said data segment, wherein said second segment checksum is formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;
- a commutative operation which operates on said second segment checksums which forms a second commutative checksum wherein flow control for the data segments is negated by the commutative operation; and
- a comparator which checks for a match between said second commutative checksum and said first commutative checksum.

Claim 12. An arrangement for forming and checking a first commutative checksum for digital data which is grouped into a number of data segments, said arrangement comprising:

- an arithmetic and logic unit,
- a first segment checksum, which is formed for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function,
- a commutative operation which forms said first commutative checksum by operating on said first segment checksums wherein flow control for the data segments is negated by the commutative operation,
- a cryptographic operation which cryptographically protects said first commutative checksum,
- a cryptographic commutative checksum formed by said cryptographic operation,

an inverse cryptographic operation to form a first commutative checksum from said cryptographic commutative checksum,

a second segment checksum which is formed for each said data segment of said digital data to which said first commutative checksum is allocated,

a commutative operation which operates on said second segment checksums which forms a second commutative checksum wherein flow control for the data segments is negated by the commutative operation, and

a comparator which checks for a match between said second commutative checksum and a reconstructed first commutative checksum, wherein said first and second segment checksum are formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function.

Claims 13-21. (canceled).

Claim 22. A method according to claim 1, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 23. A method according to claim 2, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 24. A method according to claim 3, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 25. A method according to claim 1, wherein:

said commutative operation exhibits the property of associativity.

Claim 26. A method according to claim 2, wherein:

said commutative operation exhibits the property of associativity.

Claim 27. A method according to claim 3, wherein:
said commutative operation exhibits the property of associativity.

Claim 28. A method according to claim 1, wherein said digital data and the first cryptographic, commutative checksum are archived.

Claim 29. A method according to claim 2, wherein said digital data and the prescribed cryptographic commutative checksum have been archived.

Claim 30. A method according to claim 3, wherein said digital data are secured which are processed corresponding to a network management protocol.

Claim 31. A method according to claim 1, further comprising the steps of:
protecting said digital data; and
processing said digital data in accordance with a network management protocol.

Claim 32. A method according to claim 2, further comprising the steps of:
protecting said digital data; and
processing said digital data in accordance with a network management protocol.

Claim 33. A method according to claim 3, further comprising the steps of:
protecting said digital data; and
processing said digital data in accordance with a network management protocol.

Claims 34-36. (canceled)..

Claim 37. An arrangement according to claim 10, wherein:
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 38. An arrangement according to claim 11, wherein:
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 39. An arrangement according to claim 12, wherein:
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 40. An arrangement according to claim 10 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 41. An arrangement according to claim 11 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 42. An arrangement according to claim 12, wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 43. An arrangement according to claim 10, wherein:
said digital data and the first cryptographic, commutative checksum are archived.

Claim 44. An arrangement according to claim 11, wherein:
said digital data and the prescribed cryptographic commutative checksum have been archived.

Claim 45. An arrangement according to claim 12, wherein:
said digital data and the first cryptographic, commutative checksum are archived.

Claim 46. An arrangement according to claim 10, wherein:

said digital data are protected via an arrangement of said arithmetic and logic unit; and
said digital data are processed in accordance with a network management protocol.

Claim 47. An arrangement according to claim 11, wherein:
said digital data are protected via an arrangement of said arithmetic and logic unit; and
said digital data are processed in accordance with a network management protocol.

Claim 48. An arrangement according to claim 12, wherein:
said digital data are protected via an arrangement of said arithmetic and logic unit; and
said digital data are processed in accordance with a network management protocol.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None